* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] In the access point equipment which is equipped with an interface function with the network built on a cable-transmission way, and makes data link connection with two or more mobile stations in wireless LAN area When the mobile station in said area tends to perform an authentication procedure before starting an association procedure, in order to obtain final authorization of an authentication procedure to the network administrator who manages said LAN Access point equipment characterized by having an input means by which authorization of the authentication over the mobile station which is searching for said authentication by notice means to notify that the mobile station which is searching for authentication is, and said network administrator who received said notice, or directions of refusal is inputted.
[Claim 2] In the authentication art of access point equipment which is equipped with an interface function with the network built on a cable-transmission way, and makes data link connection with two or more mobile stations in wireless LAN area From said mobile station in the 1st step to which said mobile station and said access point equipment start a predetermined authentication procedure by the authentication demand of said access point equipment HE, and said authentication procedure When said access point equipment tends to permit the authentication to said mobile station, Before answering said mobile station in the authentication response message which is the last message in said authentication procedure, while notifying final authorization of said authentication procedure to the network administrator who manages said LAN The 2nd step which starts the waiting timer for authentication which set up the maximum latency time until the last authentication is performed, Before said waiting timer for authentication carries out a time-out to said access point equipment, said network administrator by the 3rd step which directs authorization or refusal of last of authentication, and said network administrator If the last authentication authorization is directed before said waiting timer for authentication carries out a time-out The 4th step as which said access point equipment answers said mobile station considering said authentication response message as authentication authorization, The authentication art of the access point equipment characterized by completing authentication of said mobile station and starting an association procedure by performing the 5th step to which said mobile station which received said authentication response message starts the procedure of an association.
[Claim 3] The authentication art of the access point equipment according to claim 2 characterized by answering said mobile station considering said authentication response message as authentication refusal when said network administrator directs the directions which refuse authentication to said access point equipment at said 3rd step.
[Claim 4] The authentication art of the access point equipment according to claim 2 which will be characterized by answering said mobile station considering said authentication response message as authentication refusal if said waiting timer for authentication carries out a time-out before said network administrator directs the directions with which authentication is refused or permitted to said access point equipment at said 3rd step.
[Claim 5] Said authentication procedure is the authentication art of the access point equipment according

to claim 2 to 4 characterized by being the Shared Key Authentication procedure which IEEE802.11 specifies.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the access point equipment and its authentication art for preventing unjust access from the mobile station of the invader who had malice in the detail in the wireless LAN system using wireless about access point equipment and its authentication art.
[0002]
[Description of the Prior Art] In recent years, the cases where LAN (Local Area Network) is built at office, a home, etc. have been increasing in number with the explosive spread of the Internet. The advance of digital radio communication technology is also helped, from the troublesomeness of cable wiring, the needs of the so-called wireless LAN which build LAN by wireless are also increasing very much, further, it helps for the use under the migration environment in the migration terminal represented by the notebook sized personal computer to be also possible, and most number of number of spread is expected in the future. As a typical technique of this wireless LAN, there is already IEEE802.11 standardized in IEEE (Institute of Electrical andElectronics Engineers). This standardized technique has specified from the physical layer to the MAC (Media Access Control: media access control) layer in an OSI model which is a low order sublayer of a data link, can replace it with Ethernet which is the LAN transmission line of a cable, and further, although it is wireless, it is the specification which can also offer a roaming (roaming) function as an addition function of a reason.
[0003] Now, when building LAN with Ethernet of a cable etc., in order that connecting with LAN may connect a cable to a hub etc. physically, the security level of data link level is very high. That is, even if an invader trespasses upon office etc. unjustly and regards a terminal etc. as it connecting with a network, the physical activity of cable splicing is required, and it is very difficult [it] to perform it secretly, considering the arrangement situation (especially comparatively LAN of a minor scale) of general LAN. It is because the case where a hub, a router, etc. which constitute the LAN with the user of the LAN exist in the same sitting-room is most. On the other hand, in the case of a wireless LAN system, the activity of cable splicing, such as the above and Ethernet, replaces with an automatic association (Association) procedure. In systems, such as the above and existing IEEE802.11, this association procedure is a procedure for having one's existence recognized to the access point where the migration terminal is connected to backbone networks, such as a cable, and if this procedure is completed, data communication can be performed. In this procedure, the migration terminal which is present in the finite area which an access point (access point) covers will secure the security of data link level by carrying out authentication procedure of an option, before performing an association to said access point.
[0004] According to this association procedure, said mobile station When an association demand is given to said access point, The access point which was made to contain SSID (Service Set Indentifier) in the association demand message, and received this In said SSID, identify said mobile station, determine whether permit the association according to the association authorization Ruhr decided beforehand, and when granting a permission When refusing the reply message of association authorization, the reply

message of association refusal is transmitted to said mobile station. Therefore, only in this association procedure, if those who are going to have malice and are going to trespass upon a network receive even this SSID, an association will become possible simply. In order to avoid it and to perform this association procedure, the option which performs authentication procedure is formed. That is, if said migration terminal does not complete this authentication procedure, since an association cannot do it according to the method which forms the option which performs authentication procedure, data communication cannot be started but this will offer the effective function which prevents the unjust association from the migration terminal with the malice in said finite area which does not need physical connection.

[0005] In IEEE802.11, this authentication procedure is defined as a Shared Key Authentication procedure, and explains this procedure by drawing 5 and drawing 6 . Drawing in which drawing 5 shows the outline configuration of the conventional wireless LAN system, and drawing 6 are drawings showing the control sequence of the conventional authentication procedure and an association procedure.

[0006] drawing 5 -- setting -- 1 -- for a mobile station 1 and MT 4, a mobile station 2 and MT 5 is [a wireless area network and 2 / an access point AP and 3 / the mobile stations 4 and MT 7 of a mobile station 3 and MT 6] the other networks outside the wireless area network 1.

[0007] The access point AP 2 which is realized by a certain cable-transmission way and which was connected to the other networks 7 In the wireless area network 1 which the access point AP 2 covers, which exists in limited area and which consists of mobile stations MT1, MT2, MT3, and MT4 A sequence in case a certain mobile station (for example, MT1) carries out authentication procedure before an association to said access point AP 2 by actuation of switching on a power source is shown in drawing 6 .

[0008] First, a mobile station MT 1 transmits the authentication demand message 1 for starting the authentication procedure by the Shared Key Authentication approach to an access point AP 2. AP2 which received this message as AP authentication processing 8 (AP authentication processing "1") The value of Initialization Vector and Secret Key which can be decided at every authentication procedure of this at arbitration Consider as a parameter and math processing is performed according to the algorithm of WEP(Wired Equivalent Privacy) PRNG (Pseudorandom Number Generator). The value of Challenge Text it is decided that will be the meaning of 1280ctet(s) is computed, and the authentication response message 1 including this value is transmitted to a mobile station MT 1.

[0009] Next, as MT authentication processing 9 (AP authentication processing "2"), the mobile station MT 1 which received this authentication response message 1 enciphers Initialization Vector in a parameter with Shared Secret Data in the value of said Challenge Text contained the inside according to the encryption algorithm of WEP, includes the value in the authentication demand message 2 with said Initialization Vector, and answers said access point AP 2.

[0010] Furthermore, the access point AP 2 which received this authentication demand message 2 as AP authentication processing 10 (AP authentication processing "2") Initialization Vector which received the value of enciphered Challenge Text which received to coincidence, Decode based on said Shared Secret Data known beforehand, compare the result with the value of Challenge Text of the origin of the above-mentioned, and if it is the same It considers as authentication authorization, and if not the same, it will consider as authentication refusal and a mobile station MT 1 will be answered by making the result into the authentication response message 2. Then, if the result is authorization, the mobile station MT 1 which received this authentication response message 2 can go into the procedure of the next association, when it is refusal, it is authentication failure, and cannot perform association procedure.

[0011] When the access point AP 2 which received SSID (Service Set Identifier) in the association demand message from a mobile station MT 1 identifies a mobile station in said SSID, and determines whether permit the association according to the association authorization Ruhr decided beforehand, it grants a permission as above-mentioned and association processing here refuses the association response message of association authorization, it transmits the association response message of association refusal to a mobile station MT 1. In addition, the algorithm here of WEP is prescribed by RC4 technique of RSA Data Security Inc.

[0012] that is, -- according to this authentication approach -- an access point and a mobile station -- oh, the structure which an access point permits the authentication/association to a specific mobile station is realized by sharing eye ** and each other's Shared Secret Key which is secret Key. Here, a certain amount of security level is secured, without being monitored, since it is made the mounting gestalt which cannot read Book Shared Secret Key in a general user, a mobile station side prevents the theft (reading) from an invader with malice and this Key itself does not go a radio-transmission way back and forth.

[0013]

[Problem(s) to be Solved by the Invention] However, if it is in the authentication art of such conventional access point equipment, it is reservation of the security in the premise of not being unjustly stolen by those by whom the algorithm for authentication and Key for that authentication tend to have malice, and tend to trespass upon a network, and this premise cannot be collateralized 100%. That is, it is that Key stored in the memory in which no guarantee that the entire copy of the terminal which can be attested to an access point is not made is and, which cannot be accessed from the user by the formal procedure uses a special device, and cannot declare that it must have been read unjustly. Therefore, if those who are going to have malice and are going to trespass upon a network by these unjust actions are the area which an access point covers without a physical activity like the cable splicing of a cable if the association of a certain terminal can be carried out unjustly, physically, they can hide and can trespass upon a network. That is, there was a problem which is in the dead angle separated by the exterior of the closed section, i.e., a wall etc., if it is in the area which the access point which exists at the core covers by the case where a wireless network is built that the association from the terminal of those who are going to trespass upon a network with malice might be allowed, in a certain closed space (office and home).

[0014] This invention is made in view of such a technical problem, and offers the access point equipment which can raise security level by leaps and bounds, and its authentication art in a wireless LAN system.

[0015]

[Means for Solving the Problem] In the access point equipment which the access point equipment of this invention is equipped with an interface function with the network built on a cable-transmission way, and makes data link connection with two or more mobile stations in wireless LAN area When the mobile station in said area tends to perform an authentication procedure before starting an association procedure, in order to obtain final authorization of an authentication procedure to the network administrator who manages said LAN It is characterized by having an input means by which authorization of the authentication over the mobile station which is searching for said authentication by notice means to notify that the mobile station which is searching for authentication is, and said network administrator who received said notice, or directions of refusal is inputted.

[0016] The authentication art of the access point equipment of this invention In the authentication art of access point equipment which is equipped with an interface function with the network built on a cable-transmission way, and makes data link connection with two or more mobile stations in wireless LAN area From said mobile station in the 1st step to which said mobile station and said access point equipment start a predetermined authentication procedure by the authentication demand of said access point equipment HE, and said authentication procedure When said access point equipment tends to permit the authentication to said mobile station, Before answering said mobile station in the authentication response message which is the last message in said authentication procedure, while notifying final authorization of said authentication procedure to the network administrator who manages said LAN The 2nd step which starts the waiting timer for authentication which set up the maximum latency time until the last authentication is performed, Before said waiting timer for authentication carries out a time-out to said access point equipment, said network administrator by the 3rd step which directs authorization or refusal of last of authentication, and said network administrator If the last authentication authorization is directed before said waiting timer for authentication carries out a time-out The 4th step as which said access point equipment answers said mobile station considering said

authentication response message as authentication authorization, By performing the 5th step to which said mobile station which received said authentication response message starts the procedure of an association, authentication of said mobile station is completed and it is characterized by starting an association procedure.
[0017] Moreover, at said 3rd step, when said network administrator directs the directions which refuse authentication to said access point equipment, said mobile station may be answered considering the authentication response message which is the last message in said authentication procedure as authentication refusal.
[0018] Moreover, at said 3rd step, if said waiting timer for authentication carries out a time-out before said network administrator directs the directions with which authentication is refused or permitted to said access point equipment, said mobile station may be answered considering the authentication response message which is the last message in said authentication procedure as authentication refusal. Moreover, as a desirable concrete mode, said authentication procedure may be a Shared Key Authentication procedure which IEEE802.11 specifies.
[0019]
[Embodiment of the Invention] Hereafter, the gestalt of operation of the suitable access point equipment of this invention and its authentication art is explained to a detail, referring to an accompanying drawing. Drawing 1 is drawing showing the outline configuration of the access point equipment of the gestalt of operation of this invention.
[0020] The access point equipment 18 of the gestalt of this operation is replaced and installed in the access point AP 2 of said drawing 5 . That is, in said drawing 5 , in the access point AP 2 which is realized by a certain cable-transmission way and which was connected to the other networks 7, and the wireless area network 1 which the AP2 covers and which consists of mobile stations MT1, MT2, MT3, and MT4 which exist in limited area, said access point AP 2 is transposed to the access point equipment 18 shown in drawing 1 , and is constituted.
[0021] In drawing 1 access point equipment 18 In order to make wireless connection with two or more mobile stations MT1, MT2, MT3, and MT4 The radio processing means 12 which consists of the wireless strange recovery section, the baseband signaling processing section, and the data-link-control section, The antenna 19 for wireless transmission and reception connected to the radio processing means 12, A network interface means 14 to realize the function which interfaces the data which make data link connection by the other networks 7 and the cable-transmission way 17 of arbitration, and are transmitted and received by the radio processing means 12, The radio processing means 12 performs the association procedure and authentication procedure for performing data link establishment with two or more mobile stations. There Needed authentication / association processing means 13 to realize the function to exchange with the radio processing means 12 the control message exchanged for mobile stations MT1, MT2, MT3, and MT4, When authentication / association processing means 13 performs authentication processing, before permitting it finally and transmitting the message of authentication authorization to the mobile station which should carry out authentication authorization, by notifying it An authentication demand display means 16 (notice means) to realize the function which notifies the user who manages the wireless area network 1 of the existence of a mobile station which is carrying out the authentication demand by the display device, the loudspeaker, etc., After the existence of a mobile station which is carrying out the authentication demand with the authentication demand display means 16 is notified In order that the user who manages the wireless area network 1 may notify permitting or refusing it to authentication / association processing means 13, it consists of authentication input means 15 (input means) to realize the function to receive the physical input of human beings, such as a carbon button.
[0022] Hereafter, actuation of the authentication art of the access point equipment constituted as mentioned above is explained. Here, authentication procedure and association procedure are performed for a certain mobile station by powering on's etc. actuation, and a sequence in case the case where the data link connection with access point equipment 18 is established, and authentication are refused is explained.
[0023] The mobile station MT 1 in said drawing 5 should be used as the mobile station of the object

which performs authentication processing, mobile stations MT2, MT3, and MT4 should already be completed to access point equipment 18 and an association, and the data link shall be established. First, the user to whom a mobile station MT 1 manages a network in authentication procedure permits the authentication, and association procedure explains after that the case where a data link with access point equipment 18 is established, with reference to drawing 2 and drawing 4 .

[0024] Drawing 2 is drawing showing the control sequence of the authentication procedure in authentication authorization. A mobile station MT 1 transmits the authentication demand message 1 for starting the authentication procedure by the Shared Key Authentication approach to access point equipment 18 first by powering on's etc. actuation.

[0025] In access point equipment 18, authentication / an association processing means 13 by which this message was received, through the radio processing means 12 As AP authentication processing 1 (number 20 reference of drawing 2), at every authentication procedure of this The value of Initialization Vector and Secret Key which can be decided to be arbitration is made into a parameter. Math processing is performed according to the algorithm of WEP(WiredEquivalent Privacy) PRNG (Pseudorandom Number Generator). The value of Challenge Text it is decided that will be the meaning of 1280ctet(s) is computed, and the authentication response message 1 including this value is transmitted to a mobile station MT 1 through the radio processing means 12.

[0026] Next, as MT authentication processing 21, the mobile station MT 1 which received this authentication response message 1 enciphers the value of Challenge Text contained in it by making Shared Secret Data and Initialization Vector into a parameter according to the encryption algorithm of WEP, includes the value in the authentication demand message 2 with Initialization Vector, and answers access point equipment 18. In access point equipment 18, furthermore, authentication / an association processing means 13 by which this message was received, through the radio processing means 12 As AP authentication processing 2 (number 22 reference of drawing 2), the value of enciphered Challenge Text which received It decodes based on Initialization Vector which received to coincidence, and Shared Secret Data known beforehand. The result is compared with the value of above-mentioned original Challenge Text, and if it is the same, the procedure of AP authentication processing 3 (number 23 reference of drawing 2) will be performed. Processing of step S30 of the flow shown in drawing 4 - step S33 showed this procedure.

[0027] Drawing 4 is a flow chart which shows authentication processing of the above-mentioned access point. first, in this procedure, to the authentication demand display means 16, authentication / association procedure 13 of access point equipment 18 notify that it is the waiting for authentication (step S30), starts it, simultaneously the waiting timer for authentication set as the time amount of arbitration (step S31), and goes into the condition of the waiting for an authentication input (step S32). An authentication demand display means 16 by which the notice of being the waiting for authentication was received on the other hand notifies that the mobile station which is carrying out the authentication demand by the display device, the loudspeaker, etc. immediately to the user who manages a network exists.

[0028] Here, if the notice of the authentication authorization input by the input of the user who manages the network from the authentication input means 16 of authentication authorization is received before the waiting timer for authentication carries out the time-out of authentication / the association procedure 13, the authentication response message 2 which showed authentication authorization will be transmitted to a mobile station MT 1 through the radio processing means 12 (step S33).

[0029] It returns to drawing 2 , and since the result is authorization, the mobile station MT 1 which received this authentication response message 2 goes into the procedure of the next association, and transmits an association demand message to access point equipment 18.

[0030] It sets to access point equipment 18 here. Authentication / an association processing means 13 by which this message was received, through the radio processing means 12 As association processing (number 24 reference of drawing 2), in SSID in an association demand message (Service Set Identifier) When identifying a mobile station MT 1, determining whether permit the association according to the association authorization Ruhr decided beforehand and permitting it The association response message

which showed association authorization to the mobile station MT 1 through the radio processing means 12 is transmitted. If a mobile station MT 1 receives this association response message, a data link will be established between a mobile station MT 1 and access point equipment 18, and the communication link of data will be attained henceforth.

[0031] Next, when a mobile station MT 1 has the authentication refused by the user who manages a network in authentication procedure, the waiting timer for authentication carries out a time-out, and the case where authentication is refused is automatically explained with reference to drawing 3 and drawing 4 .

[0032] Drawing 3 is drawing showing the control sequence of the authentication procedure of authentication refusal / time-out case. In drawing 3 , a mobile station MT 1 transmits the authentication demand message 1 for starting the authentication procedure by the Shared Key Authentication approach to access point equipment 18 by powering on's etc. actuation.

[0033] In access point equipment 18, authentication / an association processing means 13 by which this message was received, through the radio processing means 12 As AP authentication processing 1 (number 25 reference of drawing 3), at every authentication procedure of this The value of Initialization Vector and Secret Key which can be decided to be arbitration is made into a parameter. Math processing is performed according to the algorithm of WEP(Wired Equivalent Privacy) PRNG (Pseudorandom Number Generator). The value of Challenge Text it is decided that will be the meaning of 1280ctet(s) is computed, and the authentication response message 1 including this value is transmitted to a mobile station MT 1 through the radio processing means 12.

[0034] Next, as MT authentication processing (number 26 reference of drawing 3), the mobile station MT 1 which received this authentication response message 1 enciphers Initialization Vector as Shared Secret Data in a parameter in the value of Challenge Text contained the inside according to the encryption algorithm of WEP, includes the value in the authentication demand message 2 with Initialization Vector, and answers access point equipment 18. In access point equipment 18, furthermore, authentication / an association processing means 13 by which this message was received, through the radio processing means 12 The value of enciphered Challenge Text which received as AP authentication processing 2 (number 27 reference of drawing 3) It decodes based on Initialization Vector which received to coincidence, and Shared Secret Data known beforehand. The result is compared with the value of above-mentioned original Challenge Text, and if it is the same, the procedure of AP authentication processing 3 (number 28 reference of drawing 3) will be performed. Processing of step S30 of the flow shown in drawing 4 - step S32, and step S34 showed this procedure.

[0035] first, in this procedure, authentication / association procedure 13 of access point equipment 18 notify that it is the waiting for authentication to the authentication demand display means 16 (step S30), starts it, simultaneously the waiting timer for authentication set as the time amount of arbitration (step S31), and goes into the condition of the waiting for an authentication input (step S32). An authentication demand display means 16 by which the notice of being the waiting for authentication was received on the other hand notifies that the mobile station which is carrying out the authentication demand by the display device, the loudspeaker, etc. immediately to the user who manages a network exists.

[0036] Here, if the notice of the authentication refusal input by the input of the user who manages the network from the authentication input means 16 of authentication refusal is received before the waiting timer for authentication carries out the time-out of authentication / the association procedure 13, the authentication response message 2 which showed authentication refusal will be transmitted to a mobile station MT 1 through the radio processing means 12 (step S34). Similarly, if the waiting timer for authentication carries out a time-out in the condition of the waiting for an authentication input (step S32), the authentication response message 2 which showed authentication refusal will be transmitted to a mobile station MT 1 through the radio processing means 12 (step S34).

[0037] If it returns to drawing 3 , the mobile station MT 1 which received this authentication response message 2 is not put into the procedure of the next association since the result is refusal, but there is need, what authentication went wrong to the user will be notified (number 29 reference of drawing 3 R> 3). Therefore, a mobile station MT 1 cannot perform data communication in this case.

[0038] In addition, the algorithm of WEP which has made reference here is made the same as that of the association procedure in which it is prescribed by RC4 technique of RSA Data SecurityInc., and association processing (number 24 reference of drawing 2 R> 2) is also specified by IEEE802.11.
[0039] Moreover, after the user who manages a network recognizes it that the mobile station of the waiting for authentication exists to be the time amount of the arbitration set as the waiting timer for authentication here with an authentication demand display means, in order to permit it, the user who manages a network considers as what can be set as arbitration as an appropriate value which will be converted from required time amount by the authentication input means by the time it inputs authorization.
[0040] As stated above, with the gestalt of this operation access point equipment 18 When the mobile station in area performs an authentication procedure before starting an association procedure, in order that access point equipment 18 may obtain final authorization of an authentication procedure to the network administrator who manages LAN An authentication demand display means 16 to notify that the mobile station which is searching for authentication is in area, To eye backlash which it has an authentication input means 15 by which the network administrator who received the notice directs authorization or refusal of authentication to the mobile station which is searching for authentication, and cannot be viewed physically In the wireless LAN system with malice which is easy to receive an attack of the invader of network WAKUHE in the authentication procedure before the association of a mobile station It does not perform automatically that an access point permits it, but after who views whether it is going to carry out the association, since the user who manages the network can give the authorization, he can raise security level by leaps and bounds.
[0041] Moreover, the procedure of this authentication is IEEE802.11, in the wireless LAN system which is specified as an option and which mounts the Shared Key Authentication procedure, additional mounting is required only about access point equipment, and, as for mobile station equipment, it is possible to make it function, without changing in any way.
[0042]
[Effect of the Invention] As mentioned above, according to this invention, as explained in full detail, in a wireless LAN system, security level can be raised by leaps and bounds, and mobile station equipment can be carried out, without changing in any way.

[Translation done.]